CLAIMS

1. A session-state management method comprising:

    generating an encoded session-state token, wherein the token incorporates a representation of session state of a client;

    encrypting the encoded token using a one-way encryption scheme to produce an encrypted token; and

    sending the encrypted token to the client.

2. A method as recited in claim 1, further comprising authenticating the user of the client.

3. A method as recited in claim 1, further comprising authenticating the user of the client, wherein the authenticating step comprises:

    receiving a user identification indicator ("username") and a password;

    comparing the username to a database of authorized user records, each record containing a username and a username-associated password;

    comparing the password received in the receiving step to a username-associated password of a record containing a matching username; and

    establishing a session for the user.

4. A method as recited in claim 1, wherein the generating step comprises forming a confirmation token that incorporates a representation of an incremental time block.

5. A method as recited in claim 1, wherein the generating step comprises forming a confirmation token that incorporates a representation of a current incremental time block.

6. A method as recited in claim 1, wherein the generating step comprises forming a confirmation token that incorporates a representation of an incremental time block that is prior a current incremental time block.

7. A computer-readable storage medium having computer-executable instructions that, when executed by a computer, performs the method as recited in claim 1.

8. A session-state management method comprising:

receiving a one-way encrypted, session-state token from a client, wherein the token incorporates a representation of session state of a client;

generating a one-way encrypted, confirmation session-state token;

comparing the confirmation token with the received token.

9. A method as recited in claim 8, wherein the generating step comprises forming a confirmation token that incorporates a representation of an incremental time block.

10. A method as recited in claim 8, wherein the generating step comprises forming a confirmation token that incorporates a representation of a current incremental time block.

11. A method as recited in claim 8, wherein the generating step comprises forming a confirmation token that incorporates a representation of an incremental time block that is prior a current incremental time block.

12. A method as recited in claim 8, further comprising:

issuing a one-way encrypted, replacement session-state token;

sending the replacement token to the client.

13. A method as recited in claim 12, wherein the issuing step comprises forming a replacement token that incorporates a representation of a current incremental time block.

14. A method as recited in claim 8, wherein the generating step comprises forming a confirmation token that incorporates a representation of an incremental time block, if confirmation and received tokens fail to match, the method further comprising:

generating a new one-way encrypted, confirmation session-state token, wherein the confirmation token incorporates a representation of a previous incremental time block;

comparing the new confirmation token with the received token.

15. A method as recited in claim 14, wherein the new-confirmation-token generating step comprises forming a confirmation token that incorporates a representation of an incremental time block, if confirmation and received tokens fail to match, the method further comprising:

repeating the steps of new-confirmation-token generating and comparing the new and received tokens, wherein each subsequent reiteration of such steps employs a representation of a previous incremental time block that is previous a previous reiteration of the same steps, for a specified number of times or until compared tokens match.

16. A computer-readable storage medium having computer-executable instructions that, when executed by a computer, performs the method as recited in claim 8.

17. A session-state management method comprising:

(A) receiving a one-way encrypted, session-state token from a client;

(B) generating a one-way encrypted, confirmation session-state token, wherein the confirmation token incorporates a representation of a current incremental time block;

(C) comparing the confirmation token with the received token;

(D) if the confirmation token and the received token match,

(1) issuing a one-way encrypted, replacement session-state token, wherein the replacement token incorporates a representation of a current incremental time block;

(2) sending the replacement token to the client.

if the confirmation token and the received token fail to match,

(3) generating a new one-way encrypted, confirmation session-state token using the one-way encryption scheme of the encryption step, wherein the token incorporates a representation of a previous incremental time block;

(4) comparing the new confirmation token with the received token;

(5) if the new confirmation and received tokens fail to match, then further comprising:

(i) repeating the steps of new-confirmation-token generating and comparing the new and received tokens, wherein each subsequent reiteration of such steps employs a representation of a previous incremental time block that is previous a previous reiteration of the same steps, for a specified number of times;

(ii) if, during the repeating step, the confirmation token matches the received token,

(a) issuing a one-way encrypted, replacement session-state token, wherein the token incorporates a representation of a current incremental time block;

(b) sending the replacement token to the client.

18. A computer-readable storage medium having computer-executable instructions that, when executed by a computer, performs the method as recited in claim 17.

19. A session-state management method comprising:

authenticating a user of a client to establish a session with the user;

generating an encoded session-state token, wherein the encoded token incorporates a representation of session-state of the user's session;

sending the session-state token to the client.

20. A method as recited in claim 19, wherein the authenticating step comprises:

receiving a user identification indicator ("username") and a password;

comparing the username to a database of authorized user records, each record containing a username and a username-associated password;

comparing the password received in the receiving step to a username-associated password of a record containing a matching username; and

establishing a session for the user.

21. A method as recited in claim 19, wherein:

the user is identified by a user identification indicator (UserID);

the generating step comprises forming a session-state token at least partially based upon the UserID.

22. A method as recited in claim 19, wherein:

a time block is identified by a time block identification indicator (TimeID);

the generating step comprises forming a session-state token at least partially based upon the TimeID.

23. A method as recited in claim 19, wherein:

the user is identified by a user identification indicator (UserID);

a time block is identified by a time block identification indicator (TimeID);

the generating step comprises forming a session-state token at least partially based upon the UserID and the TimeID.

24. A method as recited in claim 19, further comprising encrypting the encoded token between the generating and the sending steps.

25. A method as recited in claim 19, further comprising one-way encrypting the encoded token between the generating and the sending steps

26. A method as recited in claim 19, wherein:

the user is identified by a user identification indicator (UserID);

a time block is identified by a time block identification indicator (TimeID);

the generating step comprises combining UserID and TimeID to produce an encoded token.

27. A computer-readable storage medium having computer-executable instructions that, when executed by a computer, performs the method as recited in claim 19.

28. A session-state token generation method, wherein an authenticated user is identified by a user identification indicator (UserID) and a time block identification indicator (TimeID) identifies a specific time block, the method comprising:

combining UserID and TimeID to produce an encoded token;

encrypting the encoded token.

29. A method as recited in claim 28, wherein the combining step comprises concatenating UserID and TimeID.

30. A method as recited in claim 28, wherein the combining step comprises concatenating UserID, TimeID, and a code key.

31. A method as recited in claim 28, wherein the encrypting steps comprises encrypting the encoded token using a one-way encryption scheme.

32. A method as recited in claim 28, wherein the encrypting steps comprises:

encrypting the encoded token using a one-way encryption scheme to produce an encrypted result; and
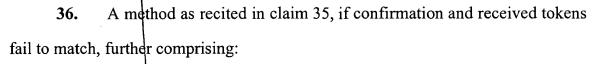
selecting a defined portion of the encrypted result to form a session-state token.

33. A computer-readable storage medium having computer-executable instructions that, when executed by a computer, performs the method as recited in claim 28.

34. A session-state management method comprising:

receiving a user-associated, encoded session-state token from a client, wherein the encoded token incorporates a representation of session-state of the user's session;

generating an encoded, confirmation session-state token;

comparing the received token with the confirmation token.

35. A method as recited in claim 34, wherein the generating step comprises forming a confirmation token that incorporates a representation of a current incremental time block, if confirmation and received tokens fail to match, further comprising:

generating a new confirmation token using a representation of a incremental time block previous of the time block representation used for the previous generating step;

comparing the new confirmation token with the received token.

36. A method as recited in claim 35, if confirmation and received tokens fail to match, further comprising:

repeating the steps of generating a new confirmation token and comparing the new and received tokens, wherein each subsequent reiteration of these steps uses a representation of a previous incremental time block that is previous a previous reiteration of the same steps, for a specified number of times or until compared tokens match.

37. A method as recited in claim 34, wherein the user-associated session-state token is encrypted.

38. A method as recited in claim 34, wherein the user-associated session-state token is one-way encrypted.

39. A computer-readable storage medium having computer-executable instructions that, when executed by a computer, performs the method as recited in claim 34.

40. A session-state management method comprising:

receiving a user-associated TimeID from a client, wherein the encoded token incorporates a representation of session-state of the user's session;

designating a first time block identification indicator (TimeID) for a first time block;

comparing the user-associated TimeID with the first TimeID.

41. The method of claim 40, further comprising:

designating a prior TimeID for a time block prior to the first time block;

comparing the user-associated TimeID with the prior TimeID.

42. A server to communicate with a client over a communications network, the server comprising:

a processor;

a session-state manager executable on the processor to:

generate a session-state token, wherein the token incorporates a representation of session state of the client;

encrypt the token using a one-way encryption scheme to produce an encrypted token; and

send the encrypted token to the client.

43. A server to communicate with a client over a communications network, the server comprising:

a processor;

a session-state manager executable on the processor to:

receive a one-way encrypted, session-state token from the client, wherein the token incorporates a representation of session state of a client;

generate a one-way encrypted, confirmation session-state token;

compare the confirmation token and the received token.

44. A server to communicate with a client over a communications network, the server comprising:

a processor;

a session-state manager executable on the processor to:

authenticate a user of the client;

generate an encoded session-state token, wherein the token incorporates a representation of session state of the client; and

send the session-state token to the client.

45. A manager as recited in claim 44, wherein session-state manager executable on the processor to encrypt the encoded session-state token.

46. A manager as recited in claim 44, wherein session-state manager executable on the processor to one-way encrypt the encoded session-state token.

47. A server to communicate with a client over a communications network, wherein an authenticated user is identified by a user identification indicator (UserID) and a time block identification indicator (TimeID) identifies a specific time block, the server comprising:

a processor;

a session-state manager executable on the processor to:

combine UserID and TimeID to produce a encoded token; and

encrypt the encoded token.

48. A server to communicate with a client over a communications network, the server comprising:

a processor;

a session-state manager executable on the processor to:

receive a user-associated, encoded session-state token from the client;

generate an encoded, confirmation session-state token, wherein the confirmation token incorporates a representation of session state of the client;

compare the received token with the confirmation token.

49. A computer-readable storage medium having computer-executable instructions that, when executed by a computer, performs the method comprising:

generating an encoded session-state token, wherein the token incorporates a representation of session state of a client;

encrypting the encoded token using a one-way encryption scheme;

sending the encrypted token to the client.

50. A computer-readable storage medium having computer-executable instructions that, when executed by a computer, performs the method comprising:

receiving a one-way encrypted, session-state token from a client, wherein the token incorporates a representation of session state of a client;

generating a one-way encrypted, confirmation session-state token;

comparing the confirmation token with the received token.